Honeywell

SECURITY NOTICE

SN 2022-11-30 #01: CLIENT AUTHENTICATION BYPASS IN LENELS2 ONGUARD (CVE-2022-37026)

This article contains:

It applies to:

OnGuard versions 7.5, 7.6, 8.0. 8.1

Executive Summary

Honeywell is aware of the vulnerability “Client Authentication Bypass” in Erlang/OTP versions before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2. The issue has been assigned the CVE-2022-37026 and rated with a severity of Critical.

Users of the LenelS2 OnGuard platform are exposed to this vulnerability through the installation/use of RabbitMQ, a third-party component within the OnGuard platform that supports communications.

Honeywell strongly recommends that users upgrade to the versions identified below or apply the proposed mitigation to resolve the vulnerability.

Honeywell

Vulnerability Synopsis

1. Client Authentication Bypass in LenelS2 OnGuard – (CVE-2022-37026)

   In Erlang/OTP before 23.3.4.15, 24.x before 24.3.4.2, and 25.x before 25.0.2, there is a Client Authentication Bypass in certain client-certification situations for SSL, TLS, and DTLS.

   CVSS Base Score: 9.8 Critical

   CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

   CVE Number: CVE-2022-37026

   https://nvd.nist.gov/vuln/detail/CVE-2022-37026

Technical Summary

See https://lists.debian.org/debian-lts-announce/2023/07/msg00012.html

Mitigation

Mitigation is strongly recommended until the appropriate upgrade is installed or if users cannot install it.

The vulnerability can be mitigated with a configuration file modification by changing the RabbitMQ advanced.config file from using “verify_peer” to “verify_none”, using the steps below:

1. On the identified Message Broker Service Host (See OnGuard System Options dialog)
2. Use Windows Services and Stop LS Message Broker service
3. Navigate to C:\ProgramData\Lnl\RabbitMQ and edit the advanced.config file as an administrator.
   - 3.1. Within the file, update the two lines…
     {verify,verify_peer},
     {fail_if_no_peer_cert,true}
   - 3.2. To a single line with the value
     {verify,verify_none}
   - 3.3. Save the updated file and start LS Message Broker service.

CAUTION: Due to the wide variety of process control equipment configurations and site-specific control strategies, it is the responsibility of each customer to assess the potential impact of this anomaly to their process & facilities.

Honeywell

Affected Products

Product	Advisory/Update
OnGuard 8.1.639	**Upgrade to OnGuard 8.1 Update 1**
OnGuard 8.0 Update 3 and earlier	**Upgrade to OnGuard 8.0 Update 4**
OnGuard 7.6 Update 3 and earlier	**Upgrade to OnGuard 7.6 Update 4**
OnGuard 7.5	**Apply mitigation steps outlined above**

Remediation

Honeywell strongly recommends that users upgrade to the appropriate version identified above. If unable, Honeywell strongly recommends that users follow the mitigation steps shown above.

References

- https://nvd.nist.gov/vuln/detail/CVE-2022-37026
- https://lists.debian.org/debian-lts-announce/2023/07/msg00012.html

Honeywell

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA. HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID HONEYWELL'S WARRANTY OBLIGATIONS.**
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.